SOFTWARECPR®
CRISIS PREVENTION AND RECOVERY, LLC

Standards Navigator

Standards Navigator Monthly Report

2-February-2015

SoftwareCPR Standards Navigator provides information and tools related to standards that play a significant role in health software and software intensive medical devices. In addition to information on existing standards, SoftwareCPR Standards Navigator keeps you up to date on new standards activity and gives you expert insight into future changes to existing standards.

http://www.softwarecpr.com/topicsframepage.htm

January 2015 Standards Navigator Overview

Medical device software

- No new documents this month.

Medical Devices

A committee draft (CD) of **IEC TR 62366-2: Medical devices – Part 2: Guidance on the application of usability engineering to medical devices** was issued for comment. This technical report provides medical device manufacturers with guidance on how to integrate usability engineering (also called human factors engineering) principles and user interface design practices into their overall medical device development processes. it focuses not only on usability as it relates to safety, but also on how usability relates to attributes such as task accuracy, completeness and efficiency, and user satisfaction. This is a companion document to IEC 62366-1 which is currently out for final (FDIS) ballot.

The draft versions of both 62366-1 and 62366-2 are available on the SoftwareCPR Standards Navigator web page.

Health IT and mobile health applications

- AAMI has filed a Project Initiation Notice with ANSI for a new standard on Application of Quality Management Principles and Practices to Health IT. The notice was published in the ANSI Standards Action publication on January 23. The notice is reproduced below.

  BSR/AAMI HIT2000-201x, Application of Quality Management Principles and Practices to Health IT (new standard)

  Stakeholders: Health IT producers, vendors, and manufacturers; healthcare providers; healthcare IT professionals; patient advocacy organizations; government representatives; and health-IT associations.

  Project Need: There is need for the application of QMS principles and practices for health software and other HIT products that pose only moderate risk to patients and that are not regulated as medical devices. HIT products differ from medical device software in that HIT complexity comes primarily from the domain content, has a very different product life cycle and tends to evolve over the life of the product. Therefore, a QMS for such HIT needs to emphasize different quality management principles.

  This standard will detail the application of Quality Management System (QMS) principles and practices for health IT software to improve patient safety.

Quality

- See Health IT.

Security

- No new documents this month.

Software Engineering and Information Technology

- A committee draft for vote (DIS) of ***ISO/IEC/IEEE 24748-4 - Systems and software engineering — Life cycle management — Part 4: Systems engineering planning*** has been circulated. The evolution of the harmonized set of ISO/IEC/IEEE 15288-12207 related standards and technical reports that are discussed in this International Standard provides detailed requirements and guidance on the application of system life cycle processes. Taken together, the parts of ISO/IEC 24748 are intended to facilitate the joint usage of the process content of ISO/IEC/IEEE 15288 and ISO/IEC 12207, Systems and software

engineering – Software life cycle processes, which in turn may be used together with related standards such as for service management, and various other lower-level process standards. In this way, ISO/IEC 24748 provides unified and consolidated guidance on the life cycle management of systems and software. Its purpose is to help ensure consistency in system concepts and life cycle concepts, models, stages, processes, process application, key points of view, adaptation, and use in various domains as the two International Standards (and others) are used in combination. It should help a project to design a life cycle model for managing progress on a project. This Part 4 focuses on the processes required for successful planning and management of the project's systems engineering effort.

The draft standard is available on the SoftwareCPR Standards Navigator web page.

- A draft technical specification (TS) of ***ISO/IEC 33050-4 - Information Technology — Process Assessment — Part 4: Process reference model for information security management*** has been circulated for vote. This Technical Specification describes a Process Reference Model for information security management with descriptions of processes. Each process of this PRM is described in terms of a purpose and outcomes, and provides traceability to requirements. The PRM does not attempt to place the processes in any specific environment nor does it pre-determine any level of process capability. (2015-4-15)

  The draft technical specification is available on the SoftwareCPR Standards Navigator web page.

- A draft technical specification (TS) of ***ISO/IEC TS 33070-4 Information technology — Process assessment — Part 4: Process capability assessment model for Information Security Management*** has been circulated. This Technical Specification provides an Information Security Management Process Assessment Model (PAM) for use in performing a conformant assessment of process capability. The PRM defined in ISO/IEC TS 33050-4 has been used as the basis for the PAM in ISO/IEC 33070-4. The processes of the PRM are described in the PAM in terms of purpose and outcomes. The PAM expands the PRM process definitions by including a set of process performance indicators called base practices for each process. The PAM also defines a second set of indicators of process performance by associating inputs and outputs with each process. (2015-4-15)

  The draft technical specification is available on the SoftwareCPR Standards Navigator web page.

- A proposal for a new work item to establish a common framework for development and usage of System Architecture has been circulated for ballot. It defines a set of processes, work products and associated terminology for the benefit of architects and other stakeholders. An outline of the proposed standard, ***Systems and software engineering — Architecture Processes*** is included in the New Work Item Proposal. (2015-4-09)

  The NP, including the outline, is available on the SoftwareCPR Standards Navigator web page.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO/IEC/IEEE 15289 FDIS	Software Engineering	Manufacturers	ISO/IEC/IEEE FDIS 15289 Software and Systems Engineering — Content of life cycle information items (documentation) The purpose of ISO/IEC/IEEE15289 is to provide requirements for identifying and planning the specific information items (documentation) to be developed and revised during systems and software life cycles and service processes. (2015-3-21)
ISO/IEC 19770-5 FDIS	Software Engineering	Manufacturers	ISO/IEC FDIS 19770-5 Information technology – IT asset management – Overview and vocabulary This International Standard provides an overview of software asset management, which is the subject of the ISO/IEC 19770 family of standards, and defines related terms.
ISO/IEC 25023 DIS	Software Engineering	Manufacturers	ISO/IEC DIS 25023 Systems and software Engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality This International Standard is a part of the SQuaRE series of international standards. It provides a set of measures for the characteristics of system/software products that can be used for specifying requirements and measuring and evaluating the system/software product quality.
ISO/IEC 19770-4 NWIP	Software Engineering	Manufacturers	ISO/IEC NWIP 19770-4 Information technology — IT asset management — Resource utilization measurement This part of ISO/IEC 19770 provides an International Standard for resource utilization measurement (RUM). A RUM is a standardized structure containing authoritative usage information about the consumption of resources that are related to the use of a software asset. (2015-3-20)

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO/IEC NWIP	Software Engineering	Manufacturers	NWIP Systems and Software Engineering- Guideline for the evaluation and selection of software engineering tools This standard is designed to provide a consistent and coherent framework for the evaluation and selection of software engineering tools. (2015-3-30)
IEC 62366-1 FDIS	Medical Devices	Manufacturers	IEC 62366-1: Medical devices – Part 1: Application of usability engineering to medical devices This standard contains the requirements for a usability engineering process for medical devices. It focusses on applying the usability engineering process to optimize medical device usability as it relates to safety.
Proposed new project	Health IT	Hospitals	Health informatics - Framework of Event Data & Reporting Definitions for the Safety of Health Software This proposal is for a new technical specification (TS) to define those data elements needed for identification of particular events including incidents, near-misses and unsafe conditions, as well as outlining good principles, relevant concepts and a process model for the recording, analysis and reporting of event-specific information related to the safety of health software.
IEC TR 80001-2-x NP	Medical devices Security	Manufacturers	IEC 80001-2-x: Application of risk management for IT networks incorporating medical devices – Part 2-x: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities. This part of IEC 80001 establishes a security case framework and provides guidance to medical device manufacturers, IT vendors and HDOs for developing, interpreting and updating security cases for networked medical devices. (2015-2-20)

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO/IEC 30130 DIS	Software Engineering	Manufacturers	ISO/IEC 30130 Software engineering – Capabilities of Software Testing Tools This International Standard defines the framework to which capabilities of software testing tools are allocated in order to identify the capabilities of products being used by any project for software testing. The framework is defined by objectives of testing, granularity of software to be tested and capabilities
ISO/IEC 25022 DIS	Software Engineering	Manufacturers	ISO/IEC DIS 25022 Systems and software Engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of quality in use This International Standard is a part of the SQuaRE series of international standards. It provides a set of measures for the characteristics of quality in use (defined in ISO/IEC 25010) that can be used for specifying quality in use requirements (in conjunction with ISO/IEC 25030) and measuring and evaluating quality in use (in conjunction with ISO/IEC 25040 and ISO/IEC 25041).
ISO/IEC 25024 DIS	Software Engineering	Manufacturers	ISO/IEC DIS 25024 Systems and software Engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of data quality This International Standard is a part of the SQuaRE series of international standards. It provides a set of data quality measures that can be used for measuring and evaluating data quality, by referring other SQuaRE series of standards, especially ISO/IEC 25012 SQuaRE – Data quality model.

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO/IEC 19770-3 DIS	Information Technology	Manufacturers	ISO/IEC DIS 19770-3 Information technology – IT asset management – Part 3: Software entitlement schema This part of ISO/IEC 19770 establishes a set of terms and definitions which may be used by the industry when discussing software entitlements (the key elements within software licenses). It also provides specifications for a file format which enables the digital encapsulation of software entitlements, including associated metrics and their management.
ISO/IEC 15026-3 DIS	Software Engineering	Manufacturers	*ISO/IEC 15026-3 Systems and software engineering — Systems and software assurance — Part 3: Systems integrity levels* This International Standard specifies the concept of integrity levels with corresponding integrity level requirements that are required to be met in order to show the achievement of the integrity level. It places requirements on and recommends methods for defining and using integrity levels and their integrity level requirements. (2015-3-20)
ISO/IEC 25066 DIS	Software Engineering	Manufacturers	*ISO/IEC 25066 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Common industry Format for Usability — Evaluation Reports* This International Standard describes the Common Industry Format (CIF) for reporting usability evaluations. It provides a classification of evaluation approaches and the specifications for the content items in an evaluation reports (content elements). (2015-4-08)

STANDARDS & GUIDANCE DRAFTS STILL IN REVIEW

These draft documents can be found on the SoftwareCPR Standards Navigator until their review period completes.

	Topic	Use / Users	Description
ISO/IEC 19770-2 DIS	Software Engineering	Manufacturers	*ISO/IEC 19770-2 Information technology — Software asset management — Part 2: Software identification tag* This part of ISO/IEC 19770 provides an International Standard for software identification (SWID) tags. The software identification tag is a standardized data structure containing identification information about a software product that supports new and automated management functions. (2015-4-08)
ISO 27799 DIS	Security	Manufacturers	*ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002* ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. The DIS can be found on the SoftwareCPR Standards Navigator web page. (2015-2-20)

REFERENCES

	Topic	Use / Users	Description
ONC 10-Year Vision	Health IT	Health IT infrastructure	*ONC 10-Year Vision to Achieve an Interoperable Health IT Infrastructure* The document can be found on the SoftwareCPR Standards Navigator web page or at http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf

BSI white paper	Medical devices	Manufacturers	*"The proposed EU regulations for medical and in vitro diagnostic devices"* The white paper can be found on the SoftwareCPR Standards Navigator web page
EC green paper	Health IT	Manufacturers	*"Green Paper on mobile Health (mHealth)"* The green paper can be found on the SoftwareCPR Standards Navigator web page
IMDRF SaMD Definitions	Software	Manufacturers	Software as a Medical Device (SaMD): Key Definitions Report on international harmonization of definitions for software as a medical device. Adopted by IMDRF in November. ***The report can be found on the SoftwareCPR Standards Navigator web page.***
Euro Commission	Medical Devices	Manufacturers	Commission recommendation of 24 September 2013 on the audits and assessments performed by notified bodies in the field of medical devices. ***The document can be found on the SoftwareCPR Standards Navigator web page.***
FDA Safety communication on cybersecurity	Security	Manufacturers and hospitals	FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations. This safety communication recommends that medical device manufacturers take steps to limit opportunities for unauthorized access to medical devices and hospitals take steps to evaluate network security and protect the hospital systems. The FDA also recommends prompt reporting of events that have impacted the performance of a medical device or hospital network.
ICS-CERT Alert regarding medical devices with hard-coded passwords	Security	Manufacturers, hospitals	ICS-CERT is issuing this alert to provide early notice of a report of a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware. The alert also identifies baseline mitigations for reducing risks to these and other cybersecurity attacks.

ONC Patient Safety Action & Surveillance Plan	Health IT safety	Health IT manufacturers, hospitals	The final version of the ONC plan that has the objectives to use health IT to make care safer and to continuously improve the safety of health IT.
ONC contract with the Joint Commission to investigate health IT-related safety events	Health IT safety	Hospitals, health IT manufacturers	The purpose of this contract is to ensure that there is an early detection system on health IT-related safety issues, including those associated with EHRs.
ONC guidance on annual surveillance plans by authorized certification bodies	Surveillance of certified EHRs	Authorized EHR certification bodies	Authorized Certification Bodies are expected to conduct surveillance on EHRs that they have certified. This guidance provides the priorities for topics to assess in the surveillance plan. Safety-related capabilities and security capabilities are two of the four areas for priority identified in this guidance.
TEAM-NB position paper on use of ISO 14971:2012	Risk management	Manufacturers	Describes the steps TEAM-NB members plan to verify where relevant if requirements of EN ISO 14971:2012 have been met. This should help manufacturers update their risk management procedures and files to maintain compliance with the Essential Requirements of the directives, when building on the presumption of conformity. ***The position paper can be found on the SoftwareCPR Standards Navigator web page.***

TEAM-NB "Vision on Revision"	Regulation	Regulators, Manufacturers, Notified bodies	This document forms the input of TEAM-NB into the debate on The Revision of European Legislation on Medical Devices. Contributions came from BSI Germany, BSI UK, DEKRA Netherlands, TUV Austria, and TUV Sud. ***The report can be found on the SoftwareCPR Standards Navigator web page.***
Report	Interoperability	Medical device manufacturers, Hospitals, Regulators	AAMI/FDA Interoperability Summit report An AAMI/FDA sponsored summit meeting on medical device interoperability was held in late 2012. This report documents the discussion and identifies themes from the summit. This report can be found at http://www.aami.org/interoperability/Interoperability_Summit_publication.pdf
Report	Wireless	Hospitals, Medical device manufacturers	AAMI Wireless Workshop report A workshop with approximately 80 invited medical wireless experts was held in late 2012. This report documents the discussion and outcomes of this workshop. A follow-up meeting is planned for March 2013. This report can be found at http://www.aami.org/wireless/2012_Wireless_Workshop_publication.pdf

Report	Security	Medical device manufacturers, Regulators	GAO report on FDA review of certain medical devices The General Accounting Office does investigations for the US Congress. In this report they reviewed how FDA reviewed implanted medical devices that used wireless communications for security vulnerabilities that could cause safety concerns. They looked at two devices that researchers had shown could be controlled by use of off-the-shelf radio devices. In their findings, they criticized FDA for not reviewing security capabilities in these devices, even though they determined that FDA had the authority to do so. This will certainly result in FDA increasing their scrutiny of security for these type of devices. Since a security vulnerability in a device that is wirelessly communicating over a network seems to surely pose a risk as well, it is likely that FDA will also increase security scrutiny of all devices that use wireless communications. Dr. Kevin Fu testified to the National Institute of Standards and Technology Information Security & Privacy Advisory Board that "Conventional malware is rampant in hospitals because of medical devices using unpatched operating systems. There's little recourse for hospitals when a manufacturer refuses to allow OS updates or security patches." A report of the meeting can be found in the MIT Technology Review http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/ The article states that “In September, the Government Accountability Office issued a report warning that computerized medical devices could be vulnerable to hacking, posing a safety threat, and asked the FDA to address the issue. The GAO report focused mostly on the threat to two kinds of wireless implanted devices: implanted defibrillators and insulin pumps. The vulnerability of these devices has received widespread press attention (see "Personal Security" and "Keeping Pacemakers Safe from Hackers"), but no actual attacks on them have been reported. Fu, who is a leader in researching the risks described in the GAO report, said those two classes of device are "a drop in the bucket": thousands of other network-connected devices used for patient care are also vulnerable to infection. "These are life-saving devices. Patients are overwhelmingly safer with them than without them. But cracks are showing," he said. (Fu was *Technology Review's* Innovator of the Year in 2009.)” One of Dr. Fu’s collaborators in research that showed an implanted defibrillator could be hacked was Dr. William Maisel who is now the Deputy Director for Science at CDRH. FDA staff has indicated that they are in the process of revising the FDA Cybersecurity Guidance. This guidance will likely include recommendations for manufacturer’s security programs for devices and additional recommendations for security information to be provided during pre-market review of devices that are intended for use on a network. In addition, the guidance is now expected to provide information on when a security issue is reportable to the FDA and when a security event will result in a recall. Another interesting bit of information in this report was the FDA response that they had hired a consultant (later determined to be McKinsey) to assess how they review software and make suggestions for improvements. This assessment is supposed to be completed by the end of 2012.

Report	Mobile medical devices	Medical devices manufacturers, Hospitals, Regulators	FCC report on Mobile Medical Devices The FCC created an independent mHealth Task Force, to research the barriers to rapid deployment of mHealth technology and develop recommendations to government and industry to address those barriers. This report documents the task force recommendations for achieving 5 goals: Goal 1: FCC should continue to play a leadership role in advancing mobile health adoption. Goal 2: Federal agencies should increase collaboration to promote innovation, protect patient safety, and avoid regulatory duplication. Goal 3: The FCC should build on existing programs and link programs where possible in order to expand broadband access for healthcare. Goal 4: The FCC should continue efforts to increase capacity, reliability, interoperability and RF safety of mHealth technologies. Goal 5: Industry should support continued investment, innovation, and job creation in the growing mobile health sector. Recommendations include: • greater collaboration with other US Federal agencies • promoting the availability of broadband for healthcare • harmonizing spectrum allocations for healthcare internationally • industry use of standards based technologies for transmitting authenticated messages and encrypted health information ***This report can be found on the Standards Navigator web page***
Report	Health IT	Hospitals, EHR vendors, MD manufacturers	Institute of Medicine report – Health IT and patient safety The Institute of Medicine produced a report on the impact of Health IT on patient safety. The report had a number of recommendations for the Secretary of HHS. ***A presentation on the recommendations and the entire report are available at the SoftwareCPR Standards Navigator web page.***

Regulation	Regulation	Medical device manufacturers, IVD manufacturers	EU draft proposed new Medical Device Regulation and In-Vitro Device Regulation These draft regulations can be found at http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf - medical devices http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_541_en.pdf - In-vitro devices

STANDARDS CURRENTLY UNDER DEVELOPMENT OR REVISION

	Topic	Use / Users	Description
IEC 62304 Amendment 1	Software Life Cycle	Medical Device manufacturers, Regulators	Amendment to the Medical Device Software Life Cycle standard. This standard is harmonized in the EU. The amendment addresses software safety classification and how to be compliant with legacy software. Current status: Comments received on the CDV are being resolved. Expected completion: 2015
IEC 82304-1	Health Software	Medical device manufacturers, Regulators	New standard on Health Software: General Requirements. This standard is intended to be for standalone software products and to cover the product level requirements such as product validation, labeling, documents to be provided to the user, etc. Current status: Comments received on the second CD are being resolved. Next step: A CDV is expected to be circulated in early 2015. Expected completion: 2015
ISO 13485	Medical devices	Medical device manufacturers, Regulators	The Quality Management System standard is being revised to bring it into alignment with ISO 9001:2008. Next step: Second DIS. Expected completion: 2016